Amendments to the Claims

This listing of claims will replace all prior versions of claims in the application:

1. (currently amended) An authentication system to verify a password, the system being arranged for coupling to a host for communication therewith, and comprising:

a first storage unit to store an authentication sequence;

a read-only memory unit to store an authentication algorithm;

a microcontroller coupled to said first storage unit~~,~~ and said read-only memory unit, ~~and a web server,~~ wherein the ~~said~~ microcontroller is configured to be coupled to and uncoupled from a host and to receive the ~~said~~ password from the host and execute the ~~said~~ authentication algorithm and wherein the ~~said~~ authentication algorithm is configured to verify the ~~said~~ password with the ~~said~~ authentication sequence; ~~and~~

a second storage unit coupled to the ~~said~~ microcontroller and configured to store data received from ~~said~~ a web server via the host and the microcontroller and wherein access by the host to data stored in the ~~said~~ second storage unit is permitted by the ~~said~~ microcontroller only if the ~~said~~ password has been verified~~,~~; and

an encoder coupled to the microcontroller and the second storage unit, wherein the encoder is configured ~~system is arranged~~ to receive encrypted data from the web server, via the host and the microcontroller ~~in encrypted form~~ and to decrypt that data before use thereof in the host if the password has been verified.

2. (currently amended) The authentication system as recited in claim 1, wherein the password is received by the ~~said~~ microcontroller from the ~~said~~ host.

3. (currently amended) The authentication system as recited in claim 2, wherein the ~~said~~ read-only memory unit is further configured to store ~~comprises~~ a shutdown algorithm configured to shut down the ~~said~~ host and the ~~said~~ authentication system after a number of incorrect passwords is received by the ~~said~~ microcontroller.

4. (currently amended) The authentication system as recited in claim 2, wherein the ~~said~~ password is received by the ~~said~~ host from the ~~said~~ web server.

5. (currently amended) The authentication system as recited in claim 1 ~~2~~, wherein the ~~said~~ authentication algorithm is hard coded on one of a group consisting of a firmware and a hardware in the ~~said~~ microcontroller.

6. (currently amended) The authentication system as recited in claim 1 ~~5~~, wherein the ~~said~~ second storage unit is a removable storage device.

7. (currently amended) The authentication system as recited in claim 6, wherein the ~~said~~ second storage unit uses flash memory.

8. (currently amended) The authentication system as recited in claim 1 ~~2~~, wherein the ~~said~~ microcontroller and the ~~said~~ read-only memory unit are implemented on a single semiconductor chip.

9. (currently amended) The authentication system as recited in claim 8, wherein the ~~said~~ first storage unit and the ~~said~~ read-only memory unit are incorporated into the ~~said~~ microcontroller.

10. (canceled)

11. (canceled)

12. (canceled)

13. (currently amended) The authentication system as recited in claim 1~~2~~, wherein the ~~said~~ authentication sequence is encrypted.

14. (currently amended) The authentication system as recited in claim 1~~2~~, wherein the ~~said~~ authentication sequence is hash-coded.

15. (currently amended) The authentication system as recited in claim 1, wherein the ~~said~~ first storage unit is located within the ~~said~~ read-only memory unit and wherein the ~~said~~ authentication sequence is hard coded into the ~~said~~ first storage unit.

16. (currently amended) The authentication system as recited in claim 1~~5~~, wherein the ~~said~~ second storage unit ~~area~~ further comprises a public storage area and a private storage area.

17. (currently amended) The authentication system as recited in claim 16, wherein the ~~said~~ first storage unit is located within the ~~said~~ private storage area ~~of said second storage area~~.

18. (currently amended) A method for authenticating a password, comprising:

~~coupling an authentication system to a host for communication therewith;~~

~~the~~ an authentication system receiving ~~the said~~ password from a host coupled to the authentication system, wherein the authentication system is configured to be coupled to and uncoupled from the host;

the authentication system receiving encrypted data from a web server~~,~~ via the host~~, in encrypted form, wherein~~ and storing ~~the said~~ encrypted data ~~is stored~~ in a storage unit of the authentication system;

the authentication system providing an authentication sequence;

the authentication system executing an authentication algorithm to verify ~~the said~~ password with ~~the said~~ authentication sequence, wherein ~~the said~~ authentication algorithm is stored on a read-only memory unit of the authentication system;

the authentication system permitting access to ~~the said~~ encrypted data on said storage unit only if ~~the said~~ password is verified; and

the authentication system decrypting ~~the~~ said encrypted data before use in the host.

19. (currently amended) The method for authenticating a password as recited in claim 18, wherein ~~the said~~ password is received by the host from ~~the said~~ web server.

20. (currently amended) The method for authenticating a password as recited in claim 18 ~~19~~, wherein ~~the said~~ password is entered into the host by a user.

21. (canceled).

22. (canceled).

23. (new) A system comprising:

a first storage unit configured to store an authentication sequence;

a read-only memory unit configured to store an authentication algorithm; and

a microcontroller coupled to the first storage unit and the read-only memory unit, and configured to be coupled to and uncoupled from a host and configured to execute the authentication algorithm to verify a password with the authentication sequence,

the microcontroller further configured to send an access request to a web server via the host if the authentication algorithm has verified the password with the authentication sequence.

24. (new) The system of claim 23, further comprising a universal serial bus (USB) connector for coupling the microcontroller to the host.

25. (new) The system of claim 23, further comprising a second storage unit coupled to the microcontroller.

26. (new) The system of claim 25, wherein the microcontroller enables the host to access data stored in the second storage unit upon verification of the password with the authentication sequence.

27. (new) The system of claim 25, wherein the microcontroller is further configured to receive data from the web server via the host and to store the data from the web server in the second storage unit.